



MONDI XHARDA

ALTERNANT CYBERSÉCURITÉ – SOC / DÉTECTION & OFFENSIF

3 SEMAINES ENTREPRISE / 1 SEMAINE ÉCOLE



+33 7 67 05 84 56



mondi.xharda@supdevinci-edu.fr



Bordeaux



21 ans / 2005



Permis B

PROFIL

Mastère Cybersécurité (Bac+4) à Sup de Vinci, certifié PJPT et CCNA SRWE. En alternance chez Dolist, j'ai déployé un SIEM Graylog en production sur un parc de 170 serveurs et industrialisé sa collecte via Ansible. Profil défensif et offensif : détection et gestion des vulnérabilités côté bleu, compromission de domaine AD et top 7 % en CTF côté rouge. Je recherche une alternance SOC ou Red/Purple Team pour 2026-2027.

CERTIFICATIONS

- PJPT – TCM Security · août 2026
- CCNA SRWE – Cisco · avril 2026
- LPIC-1 · en préparation
- PNPT – TCM Security · objectif 2027

EXPÉRIENCE

ALTERNANT – SÉCURITÉ OPÉRATIONNELLE & SUPPORT IT

DOLIST · ÉDITEUR SAAS EMAILING · BORDEAUX · MARS 2026 - SEPT. 2026

- Déploiement d'un SIEM Graylog en production : architecture 2 serveurs (Graylog/MongoDB + OpenSearch), dimensionnée pour 170 serveurs avec cible à 450.
- Tableau de bord de sécurité Active Directory : 22 widgets sur 5 onglets, et chaîne d'alerting temps réel vers Microsoft Teams.
- Automatisation Ansible : rôles Winlogbeat/Filebeat avec filtrage des logs à forte valeur de détection, playbook de gestion des clés SSH sur le parc.
- Gestion des vulnérabilités (SecPod Saner) : analyse, priorisation par criticité, suivi de la remédiation et patching.
- Supervision en production (Grafana, Prometheus) : qualification et traitement des alertes.
- Migration du datacenter : cartographie réseau et repérage des liaisons pour une bascule tracée, sans interruption de service.

FORMATIONS

MASTÈRE INFORMATIQUE – SPÉCIALITÉ CYBERSÉCURITÉ

SUP DE VINCI · 2026 – 2028

BACHELOR INFORMATIQUE (EN ALTERNANCE)

SUP DE VINCI · 2023 – 2026

BACCALAURÉAT GÉNÉRAL – OPTION NSI / SES

LYCÉE FERNAND DAGUIN · 2020 – 2023

LANGUES

- Français (bilingue)
- Anglais (professionnel)
- Albanais (natif)

RÉSEAUX



TryHackMe : mdx13



Root-Me : D - N o t e X



LinkedIn : Mondy Xharda



GitHub : mond1_d3v

COMPÉTENCES

DÉTECTION & SOC :

SIEM GRAYLOG, WAZUH · WINLOGBEAT/FILEBEAT · RÈGLES DE DÉTECTION ET ALERTING · MITRE ATT&CK · IDS SURICATA · GRAFANA, PROMETHEUS

OFFENSIF / RED TEAM :

ACTIVE DIRECTORY (BLOODHOUND, ÉLEVATION DE PRIVILÈGES, COMPROMISSION DE DOMAINE) · POST-EXPLOITATION · CTF, BUG BOUNTY

VULNÉRABILITÉS & THREAT INTEL :

CVE, CVSS, EPSS, CISA KEV · SECPOD SANER · CERT-FR / ANSSI · PRIORISATION PAR EXPLOITABILITÉ

SYSTÈMES, RÉSEAUX :

WINDOWS SERVER, ACTIVE DIRECTORY, LINUX · PROXMOX, DOCKER · PFSENSE, STORMSHIELD, VLAN, VPN IPSEC

AUTOMATISATION & DEVSECOPS :

ANSIBLE · N8N · RAG / LLM LOCAL

RÉFÉRENTIELS & CONFORMITÉ :

ISO 27001 · RGPD · NIS2

PROJETS

SENTINELIA – VEILLE ET PRIORISATION DES VULNÉRABILITÉS:

- Pipeline n8n croisant CISA KEV et EPSS pour ne remonter que les failles réellement exploitées, avec assistant RAG local (Ollama, pgvector) générant les synthèses d'analyste.

LABO ACTIVE DIRECTORY – OFFENSIF :

- Cartographie des chemins d'attaque avec BloodHound, élévation de privilèges jusqu'à la compromission complète du domaine, puis rédaction des contre-mesures.

CTF & BUG BOUNTY :

- StarHack x Yogosha : 27e / 373 (top 7 %) · Bug Bounty Yogosha 2025 · HackTheBox top 7 %.

ARCHITECTURE SÉCURISÉE – PROJET ALTHEA SYSTEMS:

- Segmentation VLAN, Stormshield, VPN IPsec, IDS Suricata et SIEM Wazuh sur environnement virtualisé.

CENTRES D'INTÉRÊT

- HackTheBox, TryHackMe, Root-Me
- Veille CERT-FR / ANSSI
- Salle de Sport
- Jeux vidéo (CS2, Call of Duty)